AMENDMENTS TO THE CLAIMS

1-45. (Cancelled)

46. (Previously Presented) A data processor for receiving and processing data to which information for tampering detection is added, said data processor comprising:

a receiver operable to receive data which includes an authentication information region for including the tampering detection information, a protected data region for including data to be subjected to tampering detection, and an unprotected data region for including data that is not to be subjected to tampering detection, wherein the protected data region includes an unprotection list which lists, by type, the data included in the unprotected data region;

a protected data authentication unit operable to detect, for the data received by said receiver, whether the data included in the protected data region has been tampered with by using the tampering detection information included in the authentication information region; and

an unprotected data authentication unit operable to authenticate, for the data received by said receiver, whether the data included in the unprotected data region is valid based on the unprotection list which has been confirmed as not having been tampered with by said protected data authentication unit.

47. (Previously Presented) The data processor according to claim 46, wherein:

the data received by said receiver is hypertext data; and

the unprotection list lists, by type, a tag included in the unprotected data region.

48. (Previously Presented) A data processor structured by a transmitting data processor and a receiving data processor, said transmitting data processor being operable to transfer, to said receiving data processor, data to which information for tampering detection is added,

wherein said transmitting data processor comprises:

an unprotection list generation unit operable to generate an unprotection list which lists, by type, data that is not to be subjected to tampering detection;

a data generation unit operable to generate data to be transmitted by arranging data to be subjected to tampering detection together with the unprotection list in a protected data region, the data that is not to be subjected to tampering detection in an unprotected data region, and the tampering detection information derived based on the data in the protected data region in an authentication information region; and

a transmitter operable to transmit the data generated by said data generation unit; and

wherein said receiving data processor comprises:

a receiver operable to receive the data transmitted from said transmitting data processor;

a protected data authentication unit operable to detect, for the data received by said receiver, whether the data in the protected data region has been tampered by using the tampering detection information in the authentication information region; and

an unprotected data authentication unit operable to authenticate, for the data received by said receiver, whether the data included in the unprotected data region is valid based on the unprotection list which has been confirmed as not having been tampered with by said protected data authentication unit.

49. (Previously Presented) The data processor according to claim 48, wherein:
the data generated by said data generation unit is hypertext data; and
the unprotection list lists, by type, a tag included in the unprotected data region.

50. (Previously Presented) A data processing method for receiving and processing data to which information for tampering detection is added, said method comprising:

receiving data which includes an authentication information region for including the tampering detection information, a protected data region for including data to be subjected to tampering detection, and an unprotected data region for including data that is not to be subjected to tampering detection, the protected data region including an unprotection list which lists, by type, the data included in the unprotected data region;

detecting, for the data received in said receiving of the data, whether the data included in the protected data region has been tampered with by using the tampering detection information included in the authentication information region; and

authenticating, for the data received in said receiving of the data, whether the data included in the unprotected data region is valid based on the unprotection list which has been confirmed as not having been tampered with in said detecting whether the data included in the protected data region has been tampered with.

51. (Previously Presented) A data processing method for transferring data, to which information for tampering detection is added, from a transmitting data processor to a receiving data processor, wherein:

in the transmitting data processor, said method comprises

generating an unprotection list which lists, by type, data that is not to be subjected to tampering detection,

generating data to be transmitted by arranging data to be subjected to tampering detection together with the unprotection list in a protected data region, the data that is not to be subjected to tampering detection in an unprotected data region, and the tampering detection information derived based on the data in the protected data region in an authentication information region, and

transmitting the data generated in said generating of the data to be transmitted; and

in the receiving data processor, said method comprises

receiving the data transmitted from the transmitting data processor,

detecting, for the data received in said receiving of the data, whether the data in the protected data region has been tampered with by using the tampering detection information in the authentication information region, and

authenticating, for the data received in said receiving of the data, whether the data included in the unprotected data region is valid based on the unprotection list which has been confirmed as not having been tampered with in said detecting whether the data in the protected data region has been tampered with.

52. (Previously Presented) A data processor for receiving and processing data with a digital signature, said processor comprising:

a receiver operable to receive the data with the digital signature from a server connected over a network;

a signer certificate acquiring unit operable to acquire a signer certificate indicating, by type, what data is signable by a signer of the data received by said receiver; and

a signature authentication unit operable to determine, when the signer certificate acquired by said signer certificate acquiring unit indicates, by type, the data received by said receiver, that a signature applied to the data is valid.

53. (Previously Presented) The data processor according to claim 52, wherein the signer certificate can include, in a list, by type, a plurality of the signable data.

54. (Previously Presented) The data processor according to claim 52, wherein:

the signer certificate can include a wildcard as a type of the signable data, and

when the signer certificate acquired by said signer certificate acquiring unit includes the wildcard as the type of the signable data, said signature authentication unit is operable to determine that the signature applied to any data received in said receiver is valid.

55. (Previously Presented) The data processor according to claim 52, wherein said signature authentication unit is operable to acquire a type of the data based on a characteristic part of a Uniform Resource Identifier of the data received by said receiver.

56. (Previously Presented) The data processor according to claim 52, wherein said signature authentication unit is operable to acquire the type of the data based on a header part of the data received by said receiver.

57. (Previously Presented) The data processor according to claim 52, wherein said signer certificate acquiring unit is operable to receive the signer certificate by using said receiver.

58. (Previously Presented) A data processing method for receiving and processing data with a digital signature, said method comprising:

receiving the data with the digital signature from a server connected over a network;

acquiring a signer certificate indicating, by type, what data is signable by a signer of the data received in said receiving of the data; and

determining, when the signer certificate acquired in said acquiring of the signer certificate indicates, by type, the data received in said receiving of the data, that a signature applied to the data is valid.